## AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 1, line 10, with the following rewritten paragraph:

This application is related to co-pending U.S. Patent Application No. ~~(Attorney Docket No. RECOP001)~~ 09/615,967 entitled SYSTEM AND METHOD FOR COMPUTER SECURITY filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. ~~(Attorney Docket No. RECOP002)~~ 09/616,805 entitled SYSTEM AND METHOD FOR GENERATING FICTITIOUS CONTENT FOR A COMPUTER filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. ~~(Attorney Docket No. RECOP003)~~ 09/615,891 entitled SYSTEM AND METHOD FOR PREVENTING DETECTION OF A SELECTED PROCESS RUNNING ON A COMPUTER filed concurrently herewith, which is incorporated herein by reference for all purposes.

Please replace the paragraph beginning on page 17, line 18, with the following rewritten paragraph:

-Figure 4 is a flowchart illustrating a process used in one embodiment to install a trap system, as in step 302 of Figure 3. The process begins with step 402 in which a trap host system is installed. In one embodiment, the trap host system is a computer, such as an Intel or SPARC computer, running the ~~Solaris~~ SOLARIS 7 operating system. In one embodiment, application programs that the user of the trap system wishes to have appear in the deception environment may be installed in the trap host system prior to the installation of the trap system software and the establishment of the virtual cage environment into which the operating system and file

system of the trap host system will be copied. In one embodiment, probabilistic data combined with random number data from a pseudo random number generator are used to determine which application programs will appear in the deception environment. In one embodiment, the nature of the business or other organization that uses the computer network influences which application programs are selected. For example, a financial institution may have different application programs, and different types of files, than a law firm.-

Please replace the paragraph beginning on page 18, line 10, with the following rewritten paragraph:

-In step 404, an administration console, such as administration console 216 of Figure 2, is installed. The administration console is a second computer system connected to the trap host system. The administration console is used to configure and control the operation of the trap host system. In addition, the administration console receives logging information from the trap host system concerning the activities of the intruder within the trap host system. In one embodiment, administration console 216 is a computer system running either a UNIX or a ~~Windows~~ WINDOWS operating system. The administration console uses its connection to the trap host system to retrieve log and configuration information for the purpose of displaying the information to the system administrator.-

Please replace the paragraph beginning on page 19, line 5, with the following rewritten paragraph:

-The process shown in Figure 4 continues with step 408 in which a network connection is made between the trap system and the router or firewall used in the computer network being protected to detect and route would-be intruders into the trap system. In one embodiment, network connections are made between the trap host system and the router or firewall for all or

selected ones of the remote access services that an intruder might use to attempt to gain unauthorized access to, or control over, a target computer or computer network. In one embodiment, the trap host system operating system is the ~~Solaris 7~~ SOLARIS 7 operating system and the remote access services for which a network connection is established include FTP (file transfer protocol), telnet, and/or other services considered to be in the so-called "demilitarized zone", or "DMZ", of the network being protected.-

Please replace the paragraph beginning on page 31, line 14, with the following rewritten paragraph:

-Figure 10 is a flowchart illustrating a process used in one embodiment to determine whether access to a particular file requested by an intruder is permitted, as in step 906 of Figure 9. The process begins at step 1002 in which it is determined whether the intruder is attempting to request a file that is at a level within the trap host system file structure that is above the highest level of the cage file structure, i.e., above the directory created to hold the file structure and operating system for the cage. For example, in one embodiment, the trap host system operating system is ~~Solaris 7~~ [[™]] SOLARIS 7. In the ~~Solaris 7~~ SOLARIS 7 operating system, the command "/../proc", for example may be used to gain access to the directory level above the file "proc", which would normally be in the highest level of the file structure for a system such as the trap host system. If an intruder were able to use this command to move above the "proc" file in the cage directory (which is a copy of the proc file of the trap host system copied into the cage directory), the intruder likely would realize that the intruder has been contained within the cage directory and, once the intruder has broken out of the cage directory, the intruder is much more likely to be able to compromise the trap host system. In one embodiment, the "/../proc" command or similar commands that might be used to access a level of the trap host system file

structure that is above the highest level of the cage file structure are filtered by a software module which recognizes such commands, prevents them from being executed, and provides an indication (as in step 1002) that an attempt is being made to move above the highest level of the cage file structure.-

Please replace the paragraph beginning on page 32, line 13, with the following rewritten paragraph:

-If it is determined in step 1002 that an attempt is being made to move above the highest level of the cage file structure, the process proceeds to step 1004 in which access to the requested file structure level is denied and an indication is provided to the intruder that the requested file does not exist, in accordance with step 908 of Figure 9. If it is determined in step 1002 that an attempt is not being made to move above the highest level of the cage file structure, the process proceeds to step 1006 in which it is determined whether the intruder is making an attempt to access a blocked network data file. For example, in the ~~Solaris~~ SOLARIS 7 operating system, all network devices have a major and minor number associated with them. It is known in the art of computer security and the art of computer hacking that files associated with certain device numbers are susceptible to being used to gain unauthorized access to or control over a target computer system. For example, in one embodiment the trap host system uses the ~~Solaris~~ SOLARIS 7 operating system for which the device files for devices that have a major number 7 and a minor number in the range of 0-7, or devices that have a major number 11 and a minor number 7, may be exploited by an intruder to gain an unauthorized level of access to or control over a target computer system. As a result, in one embodiment, it is determined in step 1006 whether the intruder is attempting to access the device files associated with a device having a major and minor number in one of the ranges listed above.-

Please replace the paragraph beginning on page 33, line 9, with the following rewritten paragraph:

-If it is determined in step 1006 that an attempt is being made to access a blocked network data file, the process proceeds to step 1008 in which access to the requested file is denied, and an indication is provided that the file does not exist in accordance with step 908 of Figure 9. If it is determined in step 1006 that an attempt to access a blocked network data file is not being made, the process proceeds to step 1010 in which it is determined whether an attempt is being made to access a process file for a process running outside of the virtual cage environment. Each computer operating system provides a way to monitor the processes or tasks currently being performed by the host system. In the ~~Solaris~~ SOLARIS 7 operating system, for example, a process table is provided in a file contained within the operating system's virtual file system. The process table is accessed by entering a file name in the directory "/proc". In one embodiment, a software module is used to filter access to the "proc" file to limit an intruder's access to files associated with processes running within the cage environment and to prevent access to processes running on the trap host system outside of the virtual cage.-

Please replace the paragraph beginning on page 2, line 6, with the following rewritten paragraph:

-Computers and networks of computers, such as local area networks (LAN) and wide area networks (WAN), are used by many businesses and other organizations to enable employees and other authorized users to access information, create and edit files, and communicate with one another, such as by e-mail, among other uses. Often, such networks are connected or are capable of being connected to computers that are not part of the network, such as by modem or via the Internet. In such cases, the network becomes vulnerable to attacks by unauthorized users, such

as so-called computer "hackers", who may be able to gain unauthorized access to files ~~store~~ stored on network computers by using ports or connections provided to connect the network to computers outside of the network.-

Please replace the paragraph beginning on page 30, line 17, with the following rewritten paragraph:

-Figure 9 is a flowchart illustrating a process used in one embodiment to keep an intruder in the trap, as in step 312 of Figure 3. The process begins with step 902 in which a request to access a file within the cage directory is received from the intruder. In one embodiment, a software module is provided to serve as a filter between requests made by an intruder to access a file, on the one hand, and the copy of the file system contained in the cage directory of the trap system, on the other hand. Such filtering software is used to prevent the intruder from accessing files that might enable the intruder to discover[[y]] that the intruder is in a trap system, and not an actual system, as described more fully below.-